

APPRISS INFORMATION SECURITY PROGRAM

Overview

At Appriss, we take the protection and security of customer data seriously. Our customers entrust us with sensitive and confidential information; thus, security is paramount in everything we do. Appriss has implemented a “security first” culture to ensure the security of data, processes and services is always top of mind.

Governance

Information security is an integral part of enterprise governance and built into strategy, concept, design, implementation and operations. Protecting critical information constitutes one of the major risks to be considered in management strategies and is recognized as a crucial contributor to success.

The Chief Security Officer (CSO) provides weekly updates on the state of security and the adequacy and effectiveness of the Information Security Program to the CIO and Business Unit Presidents. In addition, annual reports are delivered to the Executive Team detailing any significant system or data breaches and risk mitigation strategies.

Risk Assessment

The Information Security team takes necessary steps to identify internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of data or information systems.

The CSO is responsible for the development, and maintenance of the risk assessment process to be conducted on an annual basis or when there is a significant change in technology.

The IT Risk Assessment Process consists of a series of observations and interviews with management. The assessment methodology provides a risk rating for each of the technologies reviewed. The rating is established through the evaluation of the likelihood and impact of identified technology risk compared with the security controls in place. Residual risk is determined to prioritize technologies requiring heightened information security controls.

Information Security Policies

Appriss maintains a comprehensive set of Information Security Policies that are made available to all new and existing employees and contractors. Users of Appriss systems and data must agree to abide by all information security policies and a progressive discipline program is in place for policy violations.

Data Center Locations

Appriss manages multiple data center locations across each of the business units. All data center systems have 24/7 network security monitoring. Access to data centers require valid credentials and only individuals on approved access lists may enter those facilities. Data centers are monitored by video surveillance of entry and exit point access at a minimum. Visitors are required to be escorted at all times.

Database Architecture

Sensitive databases are physically separated by Business Unit and sometimes, by product. The majority of our Safety data is stored and managed across two data centers, located in Louisville, KY and Ashland, VA. Health data is stored predominately in AWS (Amazon) East/West and Retail is predominately stored across multiple data centers located in Warsaw Poland, California and Microsoft Azure. This separation, among other things, prevents a single hacking event affecting all Appriss data.

Access Control

Appriss maintains safeguards so that only authorized employees can access confidential data. We follow the principle of least privilege, an industry best practice limiting an employee's access to only the information necessary to performing his or her job. When an Appriss employee ceases employment with the company, all access is removed promptly to ensure the individual can no longer access confidential data or facilities. Mandatory employee access reviews are performed by managers on an annual basis.

Data Protection/Encryption

We leverage multiple security solutions to help prevent sensitive data from being disclosed to unauthorized individuals. When customers engage with Appriss solutions online, data in flight is encrypted, reducing the risk of exposure. In addition, when not in use, data stored in our data centers and in the cloud is encrypted, further protecting it from unauthorized access or loss.

Appriss will only transmit data or accept data through approved authenticated connections, and all users and credentials must conform to Appriss password security requirements. When data is displayed on customer-facing user interfaces, secure encrypted connections are used after customer users have been authenticated. Where possible, Personally Identifiable Information (PII) is masked based on customer need. Within the Appriss network, all customer data is encrypted at rest using storage-level encryption, and internal access to data and systems is tightly controlled and provided to Appriss employees only when required by job function based on the principle of least privilege.

Product Development Security

Security is integrated into the Appriss Software Development Life Cycle (SDLC). This includes secure coding practices, as well as both dynamic and static vulnerability testing to minimize the risk of software application vulnerabilities. Production environments are separate from development and test environments, and sensitive data is not present or used in any system within non-production environments. Changes to production systems, including the deployment of software updates and patching, go through a formal change management process, which includes security review and approvals.

Security Training

It is critical to the success of Appriss that employees have the skills and expertise to perform their job duties. Management allocates sufficient resources to train new and existing employees. Training includes but is not limited to, technical course work and certifications, attendance at industry conferences, and participation in industry working groups.

All employees are trained at least annually regarding the policies for Information Security and the protection of confidential data and systems. Once every two years, all employees with access to Safety systems are required to take CJIS (Criminal Justice Information Security) online training.

Technical Security Testing

Appriss conducts monthly internal vulnerability scans and web application code reviews. The security team utilizes scanning tools and manual methods to test systems for vulnerabilities. Results of testing are provided to all business unit IT teams and remediation work, if necessary, is scheduled and implemented during maintenance periods. Annual third-party external penetration and network assessments are performed, and summary results are available upon request.

System and Application Patching

Vulnerabilities identified through scanning tools or via alert bulletins will be reviewed weekly. All confirmed critical and high-risk vulnerabilities must be reviewed, patched or mitigated according to the appropriate Appriss business unit standard. Emergency patches may be applied immediately and directly to production. All other patches are applied in development and QA prior to updating production. At no time may a critical patch be delayed more than 30 days.

Incident Response

The Appriss security team is comprised of professional security analysts that maintain world class security certifications like the CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker), CRISC (Certified Risk and Information Systems Control), etc. The team is capable of comprehensive incident management and investigations.

Appriss utilizes a 3rd party security partner to provide first level threat detection and incident management with 24/7 security monitoring and threat analysis across all business unit networks. Alarms are configured to notify the security team when defined thresholds are crossed. The security team investigates and responds to all passive and direct attacks on any Appriss system.

Additionally, the security team monitors internal and external activity in order to respond and mitigate newly discovered threats proactively. This includes, but is not limited to:

- Unusual File Additions, Deletes or Changes
- Access Control Changes
- Privileged Account Usage
- Failed Login Attempts
- Blocked Access Attempts
- Suspicious Traffic and Location Activity
- Unusual Access Attempts

Compliance

The design, operation, use, and management of information and information assets are subject to statutory, regulatory, and contractual security requirements. Compliance with legal requirements is necessary to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. Legal requirements include, but are not limited to: state statute, statewide and agency policy, regulations, contractual agreements, intellectual property rights, copyrights, and protection and privacy of personal information.

Each business unit at Appriss provides SaaS and service solutions to different types of organizations. Varying types of data elements across the enterprise requires Appriss to align with multiple types of security frameworks and compliance requirements.

Retail

International Organization for Standardization (ISO27001) - Appriss Retail products and services meet the physical and technical standards and provide all necessary controls for our customers to maintain their administrative security compliance standards. Specifically, Appriss Retail utilizes ISO 27001 to guide its overall Information Security Controls to reasonably protect the confidentiality, integrity, and availability of the confidential information that it creates, receives, maintains, or transmits on behalf of our customers. Furthermore, Appriss agrees to report any security incident to our customers of which it becomes aware within 48 hours.

Safety

SOC for Service Organizations (SOC2 Type2) - Appriss Safety solutions are required to conduct annual SOC2 Type2 reporting from a certified CPA firm. This rigorous review requires Appriss to present approximately 500 pieces of evidence that our security controls are operating as intended.

Criminal Justice Information System Policy (CJIS) - Appriss recognizes and uses the CJIS Policy to guide its control environment for the Safety Business Unit. Aside from the technical control environment, Appriss requires all employees and contractors to pass a criminal background and fingerprint check.

Health

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) - The Office for Civil Rights enforces the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, which requires “covered entities” and “business associates” to provide notification following a breach of unsecured protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety. Appriss may be considered a “business associate” with some services offered to “covered entities” and will agree to review and sign Business Associate Agreements, as required.

Conclusion

Appriss takes utmost care in the administration of its data security protocols, always mindful of the sensitive information with which it has been entrusted by both government and private entities in our Safety, Health, and Retail sectors. Further, Appriss is diligent in its protection of employee information and is careful to minimize the amount of employee data it collects, as well as to maximize security controls over that information. Appriss is committed to further strengthening its data security program to respond to future changes in the regulatory landscape and to best respond to customer and consumer demands.